



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/538,951	03/31/2000	Carl M. Ellison	0423903.P8097	9459

8791 7590 05/07/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN  
12400 WILSHIRE BOULEVARD, SEVENTH FLOOR  
LOS ANGELES, CA 90025

EXAMINER
----------

STULBERGER, CAS P

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 05/07/2004

18

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/538,951

Applicant(s)

ELLISON ET AL.

Examiner

Cas Stulberger

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 March 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 6-13, 15-17.
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: \_\_\_\_.

**DETAILED ACTION**

***Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 6, 16, and 19-20 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No 5,825,880 to Sudia et al.

3. In regards to claims 1, 6, and 19, Sudia discloses a “certificate signing unit” (CSU), which is a tamper-proof secure module” (Sudia: column 1, lines 49-51). This meets the limitation of “stored in hardware-protected memory.” “The CSU generates its public/private signature key pair internally” (Sudia: column 1, lines 54-55). This meets the limitation of “generating an attestation key pair within a platform.” “The private signature key is confined securely and permanently inside an area of the device that cannot be read externally, and outputs only the corresponding public key, which is used to verify signatures” (Sudia: column 1, lines 55-59). Sudia also discloses that “public key certificates are electronic documents signed by a trusted issuer and used to attest to the binding of a user’s name to a public key and other related data. Certificates provide assurance to the public that the public key is identified in the certificate and is owned by the user whose name is on the certificate. Sudia also discloses that each signing device has an electronic certificate, signed by the manufacturer containing: the devices’ public signature verification key, and the device’s public encryption key” (Sudia: column 9, lines 49-

52). This meets the limitation of “producing a certificate including a public attestation key to attest that a private attestation key, corresponding to the public attestation key.”

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 2, 10-15, and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,825,880 to Sudia et al as applied to claims 1, 10, 15, and 19 above, and further in view of U.S. Patent No. 4,403,283 to Myntti et al.

6. In regards to claims 10-15, Sudia discloses “the message server includes a system log that maintains an audit trail of messages and documents sent to and from the signing device” (Sudia: column 7, lines 57-60). This meets the limitation of “a device in communication with the processor, the device to store an audit log, the audit log being a listing of data or presenting information loaded into the isolated area of the system memory.” Sudia however does not disclose “a processor running in isolated execution mode.”

Myntti discloses that “each user program is ‘isolated’ from execution of each other user program. Each user program executed by the processor can be executed independently of the memory requirements of any other user program executed by the processor” (Myntti: column 6, lines 19-28). This meets the limitation of “a processor running in isolated execution mode.”

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of generating key pairs as disclosed by Sudia with the method of the processor running in isolated execution mode as disclosed by Myntti in order to “avoid memory shortage problems resulting from computing systems wherein there is inadequately regulated or unregulated memory contention among various user programs” (Myntti: column 5, lines 61-65).

7. Claims 3-5, 7-9, and 22-23, are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,825,880 to Sudia et al as applied to claims 1, 10, 15, and 19 above, and further in view of U.S. Patent No. 6,609,199 B1 to DeTreville.

8. In regards to claim 3, 4, 22, and 23 Sudia does not disclose “producing the certificate at initial power-on.” DeTreville discloses that during authenticated boot the “CPU maintains a ‘boot log’ to track software modules and programs that are loaded” (DeTreville: column 6, lines 56-64). DeTreville also discloses that “the CPU can generate a signed certificate containing the boot log data to attest to the particular operating system (including drivers) that is running” (DeTreville: column 9, lines 5-13). This meets the limitation of “producing the certificate occurs at an initial power-on of the platform.”

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of producing a certificate to attest to the private key is stored in hardware-protected memory as disclosed by Sudia with the method of generating a certificate at power-on of the platform as disclosed by DeTreville in order to “make a signed

attestation of the current value of any arbitrary region of memory and/or a register” (DeTreville: column 9 lines 30-31).

9. In regards to claim 5, Sudia discloses “signing devices encrypt their communications using a public/private cryptographic scheme” (Sudia: column 9, lines 55-56). This meets the limitation of “wherein the producing of the certificate further comprises encrypting the public attestation key with a private key held by the agent.”

10. In regards to claim 7-9, Sudia discloses “sending a hash of its firmware and signing the hash value using its device signature key and sending the signed hash value to the other devices” (Sudia: column 10, lines 10-14). This meets the limitation of “a hash value of an audit log” and “wherein the hash value is signed with the private attestation key.” However Sudia does not disclose “a challenge and response using a nonce.”

DeTreville discloses challenge and response using a nonce (DeTreville: Figure 14, 15). It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of the method of a signing system to affix a signature as disclosed by Sudia with the method of sending a challenge nonce to the application as disclosed by DeTreville in order to verify the public key for the application and initiate trusted communication between the device and the application (DeTreville: column 23, lines 35-40).

11. In regards to claim 18, Sudia discloses “the signing device generates an unsigned certificate. The certificate the signing device’s identity and the public signature verification key

Art Unit: 2132

for the device's signature key. The key, which is to be recertified, is the same public key, which was originally generated by the device at the start of the protocol. The device signing key and its associated manufacturer's certificate remain unchanged during this process, and are retained permanently as proof of the device's origin and underlying characteristics" (Sudia: column 14, lines 3-17).

12. Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,825,880 to Sudia et al as applied to claims 1, 10, 15, and 19 above, and further in view of U.S. Patent No. 6,108,644 to Goldschlag et al.

In regards to claims 8 and 9, Sudia does not disclose challenge and response. Goldschlag discloses "a hashed combination of the once, audit secret, and salt" (Goldschlag: column 8, lines 59-63; column 9, lines 2-5).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of a signing system to affix a signature as disclosed by Sudia with the method of challenge and response as disclosed by Goldschlag in order to deter the illicit sharing of certificates (Goldschlag: column 9, lines 36-37).

### ***Conclusion***

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cas Stulberger whose telephone number is (703) 305-8034. The examiner can normally be reached on Monday - Friday, 9:00A.M. - 5:00P.M.


Art Unit: 2132

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CS

CS

  
GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100